WRITTEN BY

LGP

2025 CYBER-SECURITY COMPLIANCE

The 2025 amendment to the Cybersecurity Act, aligned with the EU NIS 2 Directive, introduces significant changes to how businesses must respond to cyber incidents. To clarify the legal obligations and best practices for companies, we consulted JUDr. Martin Jacko, Partner at Lansky, Ganzger, Jacko & Partner.

MARTIN JACKO
Attorney at law and Managing Partner Lansky, Ganzger, Jacko & Partner s. r. o.

JUDr. Martin Jacko, attorney at law and managing partner of Lansky, Ganzger, Jacko & Partner (Bratislava and Prague), in addition to cybersecurity, focuses primarily on strategic consulting, crisis management, restructuring/insolvency, corporate acquisitions, and large construction and infrastructure projects at both national and international levels (including FIDIC contracts) and international sanctions. He also serves as a bankruptcy and restructuring trustee, a member of the Antimonopoly Office of the Slovak Republic's Board, and an active board member of the Slovak Compliance Circle, which he represents in the Rule of Law initiative.

LGP

How should a company start protecting itself against cyber threats?
First and foremost, every company should conduct an impact analysis to determine whether it falls under the scope of the Cybersecurity Act. To do so, it's necessary to assess in detail the specific sector in which the entity operates, as well as whether it meets the definition of a small or medium-sized enterprise and possibly other criteria. I would like to highlight that the law applies to a relatively wide range of companies.

If an entity finds that it is subject to this regulation, it must register within 60 days of starting the relevant activity (or from the effective date of the law if the activity is already being conducted, which will be the case for most). Registration should be in the list of essential service operators maintained by the National Security Authority of the Slovak Republic (NBÚ). After registration, it is necessary to conduct a risk analysis and a GAP analysis to identify deficiencies and adopt measures to ensure compliance with the Cybersecurity Act. These measures must then be implemented within 12 months of registration, and a cybersecurity audit must be conducted within 24 months.

However, even if a company does not fall directly under the regulation of the Cybersecurity Act, we strongly recommend implementing at least basic standards such as two-factor authentication, the principle of least privilege, regular software updates, and employee training.

> **We consider cybersecurity to be a multidisciplinary topic, where cooperation between various professions is essential.**

If a company faces a cyberattack, what are its legal obligations?
In the event of a cyber incident, it must be addressed immediately, evidence must be secured, and it should be reported to the Computer Security Incident Response Team (CSIRT) or the NBÚ.

Under the Cybersecurity Act, there are several reporting obligations:
- Early warning (within 24 hours of the incident),
- Incident notification (within 72 hours),
- Interim report (upon CSIRT request),
- Final report (within one month of notification).

If personal data is compromised during the attack, the company must notify the Office for Personal Data Protection within 72 hours in accordance with GDPR. Failure to meet these obligations can result in significant fines, either under the Cybersecurity Act or GDPR.

What role does employee training play in cybersecurity?
Training is crucial for both employees and management. The Cybersecurity Act requires regular employee training, which must be ensured by the company's statutory body. Regular training, phishing attack simulations, and testing incident responses reduce the risk of a successful cyberattack. Therefore, it is recommended to invest not only in technical measures but also in regular training to help employees recognize potential threats and minimize the risk of cyber incidents. Failure by the statutory bodies to fulfill these obligations can have serious legal consequences, such as personal liability for damages (under the provisions of the Commercial Code—failure to act with due care), as well as disqualification or restriction of membership in the statutory body for a certain period or other sanctions, such as fines.

How is the role of a lawyer changing in providing legal services in the field of cybersecurity?
To properly provide legal services in the field of cybersecurity, it is primarily necessary to have good cooperation with other experts in this area, as well as knowledge of certain technical terms and processes within the IT sector. We consider cybersecurity to be a multidisciplinary topic, where cooperation between various professions, such as IT experts, auditors, risk management specialists, and, of course, legal/compliance experts, is essential.

That is why at Lansky, Ganzger, Jacko & Partner, s. r. o. (law), we have created a unique partnership with companies such as Moore BDR s. r. o. (cybersecurity audit), DXC Technology Slovakia s. r. o. (IT), and Aon Central and Eastern Europe (insurance), to provide comprehensive services in the field of cybersecurity. In this area, the lawyer's role should mainly consist of coordinating the entire process and thoroughly reviewing internal processes to propose recommendations aimed at ensuring compliance with applicable legal norms.